AFRL-IF-RS-TR-2005-93
Final Technical Report
March 2005

OPTIMAL AIDE SECURITY INFORMATION SEARCH (OASIS)

BAE Systems Enterprise Systems, Inc.

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2005-93 has been reviewed and is approved for publication

APPROVED: /s/
                 BRIAN T. SPINK
                 Project Engineer

FOR THE DIRECTOR: /s/
                           WARREN H. DEBANY, JR.
                           Technical Advisor
                           Information Grid Division
                           Information Directorate

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE March 2005	3. REPORT TYPE AND DATES COVERED Final Sep 02 – Aug 04

4. TITLE AND SUBTITLE OPTIMAL AIDE SECURITY INFORMATION SEARCH (OASIS)	5. FUNDING NUMBERS C - F30602-99-D-0001/0013 PE - 33140F PR - 7820 TA - JM WU - 13
6. AUTHOR(S) Chetna Kapadia	

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) BAE Systems Enterprises Systems, Inc. 111 E. Chestnut Street Rome NY 13440	8. PERFORMING ORGANIZATION REPORT NUMBER N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFRL/IFGA 525 Brooks Road Rome NY 13441-4505	10. SPONSORING / MONITORING AGENCY REPORT NUMBER AFRL-IF-RS-TR-2005-93

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Brian T. Spink/IFGA/(315) 330-7596   Brian.Spink@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT *APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.*	12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 Words)*
The purpose of the Optimal AIDE Security Information Search (OASIS) effort was to investigate and prototype a tool that can assist the network security analyst in collecting useful information to defend the networks they manage. The resulting tool allows the collection of threat, vulnerability, and countermeasure data from multiple web sites that are further processed to eliminate duplication. The scope of the work encompasses the design and implementation of a Graphical User Interface (GUI) to control the search and collection of data relating to user-defined topics. This included the integration of a Government Off-The-Shelf (GOTS) tool to perform the actual search. The effort put forth on this project has demonstrated that it is feasible to support network security analysts with an automated tool to quickly collect, view, and act on information that can protect an information system network.

14. SUBJECT TERMS Threat, vulnerability, countermeasure data	15. NUMBER OF PAGES 46
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

TABLE OF CONTENTS

List of Exhibits

1.0 SUMMARY

One of the greatest challenges facing those who are tasked with keeping information networks secure is obtaining timely, pertinent, and accurate information to perform the work. New software vulnerability alerts are discovered and posted on the Internet every day that could be of interest to a network defender. These sources provide useful information about potential vulnerabilities, including threat ratings, analysis by other security experts, reports of attacks and how they were neutralized, and ways to harden software or hardware to minimize or eliminate vulnerabilities. The challenge for network defenders is navigating this sea of information and locating the important elements that can help to keep their networks secure.

The Optimal AIDE Security Information Search (OASIS) project was envisioned to address the needs of the network defender by assisting in the collection of threat, vulnerability, and countermeasure data from multiple data sources (i.e., web sites). The search results could then be processed to eliminate duplicate information, combined into a concise useful format, and presented to a user with reference links to access additional information. As a result, the network defender would have a tool to quickly view pertinent information and take necessary actions to protect the network.

There are two major thrusts of research and development associated with the OASIS objective. The first addresses the Information Search capabilities that are the focus of the work documented in this Final Technical Report. The second thrust is Information Extraction, which will be developed in a following effort.

The Information Search capabilities were developed using Java to create a Graphical User Interface (GUI). The GUI allows the user to organize the security search topics into a tree structure, which can easily grow and shirk by adding or removing topics from the tree. The tree content can be saved in the text file and retrieved in the GUI with little or large modifications in the topics or its organization.

The GUI was integrated with a Government Off-The-Shelf (GOTS) tool named "Buddy" to perform the Internet search on the specified security topic. The results of the search are displayed in a frame where the user may select one of the search result hyperlinks and view the corresponding web page in another frame within the GUI.

Some of the options the tool provides include the flexibility of downloading html pages corresponding to the search results at a later time when the system usage is low. These downloaded html pages will enable the user to continue functioning in the event that the network is down and the Internet is not available. The GUI also provides an option to perform an Internet search on a currently selected topic or all of the security topics in the tree, whenever desired, in order to obtain the most recent information available on the Internet.

The field of information extraction is still in the research and primitive stage. Writing the software that makes computers understand the content of html (or even text) documents, and interpret the information to eventually summarize or combine the information extracted from multiple sources into a single document is a difficult task. It is possible to extract the static

information from the web site with the help of tools such as the one developed by Fetch Technologies Inc. However, it involves a good deal of user intervention in order to train the tool to extract the desired information, especially in the form of a list or some number of lines of text situated on a specific web page at the specified location. It is recommended that the Fetch tool be further investigated and analyzed to try to customize it to meet some, if not all, of the requirements of OASIS.

2.0 INTRODUCTION

Network security is a constant process that requires considerable time and effort just to keep current with all of the pending threats. Network security analysts need to repeatedly check favorite web sites for news and software patches, and to review e-mails received from the various mail lists to prepare the network to face new threats. This enables the security analyst to stay current with what is happening both on the internal network as well as in the outside world. Additionally, keeping up with current issues on a daily basis makes it much easier to stay aware of the software patches that must be downloaded and installed.

The abundance of information that can be found on the Internet regarding any security topic is overwhelming. Web sites often have several reference links to other relevant sources. For instance, if a user visits the Symantec web site on a daily basis, s/he will find links on security topics such as Latest Threats, Advisories, Virus Definitions, Security Updates, etc. The amount of time needed to manually read this information to identify new threats, advisories, or updates to existing security vulnerabilities and patches is enormous. However, collecting the information and trying to interpret it is only part of the task. The network security analyst must ascertain how it applies to the network s/he is managing and how to use the information to secure the network.

Moreover, changes in network security information and its sources are unpredictable. The voluminous amount of information the analyst relies on may not change for days or months, yet at other times, it may change rapidly when someone discovers a new threat. There will be times when the web site administrator changes the organization of the information or changes the URL. Furthermore, there is the possibility that the web site might be removed, thus making the previously relied on information no longer available. Searching for reliable network security information is further complicated by the repetition of information among the various web sites. The user must decide if the information is repeated and, therefore, safe to ignore.

OASIS was envisioned to provide the network security analyst with a tool to help alleviate the burdensome task of searching for relevant network security information over the Internet. The software was developed to assist the network security analyst in automating the tedious tasks presented above and to provide a collaborative tool to help organize cyber security information; maintain a list of contacts, a calendar of events, and lists of tasks to accomplish, along with saving and restoring the important security information.

Consequently, the goal was to develop software that serves as a search engine to extract intrusion detection information from the pre-selected security web site(s), and presents the consolidated information in a simplified view. This goal was translated into the following set of primary objectives to achieve in developing the OASIS software.

1. Develop the OASIS software using Java.

2. Make the software design modular enough to restrict future modifications to specific modules or involve the addition or deletion of modules.

3. Provide the appearance and functionality of a collaboration tool such as Microsoft Outlook.

4. Provide the ability to "drag and drop" the search results into a "personal folder" or a "deleted items folder".

5. Indicate to the user the latest security updates by displaying a flag mark in the GUI near the relevant security topic or by displaying a pop-up message dialog.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

This section presents the methods, assumptions, and procedures developed for the OASIS software.

3.1 INPUT/OUTPUT FILES

All data processed by the OASIS software are stored in files. The file formats used are text and html. The tree representation of the security topics is stored in a text file. The default file that is initially loaded by the software is called "topics.txt" using the format - N,TopicString, where, N is a number indicating the level of the TopicString in the tree starting with number zero for the root node, and the TopicString is the description of the search topic at that level. Note that there is no white space before and after the comma (,). Moreover, no white space is allowed at the end of the text file.

After the tree is loaded into the GUI from the "topics.txt" file, it can be modified by adding, deleting, or renaming the nodes. These modifications can be saved to the same text file in the format described above or saved as a different text file.

The results of the Internet search executed using the Buddy are stored in an html file with the extension ".htm". This html file is referenced as a results file in this document. The results file containing a list of hyperlinks, along with a brief summary of information contained in the web page corresponding to that hyperlink, is created for each security topic. For each security topic, there could be zero or more html pages downloaded (referenced as downloaded files) corresponding to a number of hyperlinks in the results file. The name of the results file is generated by concatenating the words in the security topic phrase and removing white spaces. The name of the downloaded file is generated by concatenating the words in the hyperlink URL and replacing special characters including slash, comma, dollar sign, etc. with an underscore.

For example, if a search on the security topic "war dialing" returns two hyperlinks, then the corresponding results file will be created with the name "wardialing.htm". If one of the hyperlinks URL is http://encyclopedia.thefreedictionary.com/War%20dialing, then a downloaded file will be created with the name "encyclopedia_thefreedictionary_com_War_20_dialing.html". Note that the extension used for naming the downloaded file is ".html". The downloaded file becomes useful in the event the Internet is off-line and the user needs to access the information on a specific security topic. This assumes that the downloaded files were generated for that topic prior to the Internet going off-line.

The GUI provides the functionality of open, save, save as, and download files.

3.2 SOFTWARE DEVELOPMENT TOOLS

This software was developed using Java version 1.4.2. This version of Java includes the support for Swing GUI components. Swing is a large set of components ranging from the very simple, such as labels, to the very complex, such as tables, trees, and styled text documents. Swing provides extensive support and customization capabilities for the GUI components.

The software was implemented using NetBeans IDE version 3.4.1, an open source Integrated Development Environment (IDE) for the Java software developer. NetBeans offers the tools to develop cross-platform desktop, mobile, and web applications.

3.2.1 KEY SWING GUI COMPONENTS USED

JTree

For the OASIS GUI, the security topics are organized into a tree structure using the JTree component. The JTree object does not actually contain the data; it simply provides a view of the data. The JTree gets the data by querying its data model. JTree displays its data vertically (see Exhibit 3-1). Each row displayed by the tree contains exactly one datum, which is called a node (also referenced as topic node in this document as node represents the security topic for this application). The tree has a root node from which all nodes descend. A node can either have children or not. Nodes that cannot have children are leaf nodes. In Exhibit 3-1, "Security Analyst Assistant" is a root node. "Security Topics" is a node with children (also known as a non-leaf node). "Tasks" is a leaf node.

The GUI provides the functionality of basic tree operations – add, insert, remove, and edit nodes.

Note that the portion of the tree shown in Exhibit 3-1 is considered a fixed part of the tree. The following restrictions are implemented to make it a fixed tree part.

❑ No node can be added to the root node,. i.e., "Security Analyst Assistant". In other words, no nodes can be inserted into any of the children of root node.

❑ The root node cannot be removed or renamed.

❑ None of the children of the root can be deleted or renamed.

Exhibit 3-1   Basic Tree
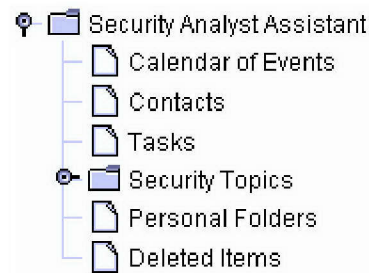
Exhibit 3-2 shows the non-leaf node "Security Topics" as partially expanded. This demonstrates how a node is updated when a user opens a new topics file, and how the descendents of this node are saved to a text file when the tree is saved. The fixed part of the tree is not affected during these two operations.

Exhibit 3-2   Expanded Tree

DefaultMutableTreeNode

A DefaultMutableTreeNode is a general-purpose node in a tree data structure. A tree node may have at most one parent and zero or more children. The DefaultMutableTreeNode provides

operations for examining and modifying a node's parent and children as well as operations for examining the tree of which the node is part.

For a security topics tree in the OASIS GUI, the name of the topic that appears at the node is actually a user object of type DefaultMutableTreeNode. Note that this user object points to data associated with the topic node. In other words, the user object is not only the topic name as it is seen in the tree but a tuple of <topic name, results file>. Remember, the results file is the html file generated as a result of the Internet search performed on the topic name. It is due to this association, when the user selects a topic node in the GUI, that the corresponding results file is displayed in the top frame of the right pane. For example, in Exhibit 3-2, the user object for a leaf node "Cert CC Advisories" is tuple <Cert CC Advisories, CertCCAdvisories.htm>, whereas for a non-leaf node "Advisories" the user object is tuple <Advisories, null>.

Notice that the GUI displays the corresponding results file when a security topic at a leaf node is selected, but when a security topic at a non-leaf node is selected, a list of its children is displayed.

DefaultTreeModel

The DefaultTreeModel provides the methods for accessing a specific node of the tree, retrieving the number of children of a particular node, determining whether a node is a leaf, notifying the model of a change in the tree, and adding and removing tree model listeners.

When a tree is initially created in a GUI after reading the topics and levels information from the "topics.txt" file, or because of the add/insert node operation, the insertNodeInto( ) method of DefaultTreeModel is used. Similarly, for removing a node from the tree, the removeNodeFromParent( ) method is used. If the DefaultTreeModel does not apply to the software domain, then it is possible to define a custom TreeModel.

JToolBar

The JToolBar provides a useful component for displaying commonly used actions or controls. It allows the grouping of several other components, usually buttons with icons, into a row or column. The tool bars often provide easy access to functionality that is also accessible through the menus.

For the OASIS GUI, the tool bar items that are implemented are shown in Exhibit 3-3. For an explanation of each tool bar item, refer to Appendix A, User's Guide.

It is possible to hide/view the tool bar by selecting the Toolbar menu item from the View menu. Each tool bar icon has an action associated with it, which will be performed upon its selection.

Exhibit 3-3   Tool Bar

JMenuBar

A menu provides a space-saving way to let the user choose one of several options. Menus are not placed with the other components in the GUI. They usually appear either in a menu bar or a pop-up menu. A menu bar contains one or more menus. A pop-up menu is a menu that is invisible until the user makes a selection. Exhibit 3-4 shows the menu bar implemented for the OASIS GUI. The JMenu objects File, Edit, View, etc. are added to the menu bar to construct a menu. When the user selects a JMenu object, its associated JPopupMenu is displayed allowing the user to select one of the JMenuItems on it. Exhibit 3-5 shows a JPopupMenu for the Edit JMenu object.

Exhibit 3-4   Menu Bar

Exhibit 3-5   Menu Bar Pop-up
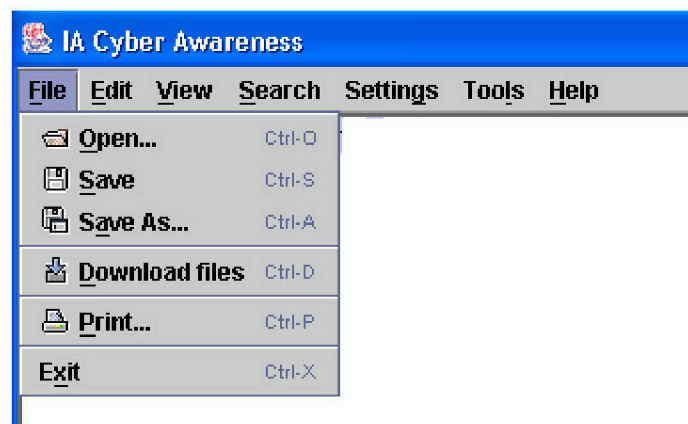
3.2.2   EVENTS AND EVENTS LISTENERS USED

Events occur any time a key or mouse button is pressed. Swing components can generate many different types of events. Each event type is represented by an object that, at the very least, identifies the source of the event. Some events carry additional information such as an event type, name and identifier, and information about the state of the source before and after the event was generated. The source of an event is most commonly components or models (e.g., Hyperlink and TreeModel) but different kinds of objects can also generate events.

In order to receive notification of events, the object needs to register listeners with the source object. To register a listener use the addXXListener( ) method; to unregister a listener use the removeXXListener( ) method, where XX is a placeholder for the name of the event or action generated by the swing component.

The following describes the key events and listeners handled by the OASIS GUI.

9

TreeSelectionEvent and TreeSelectionListener

The TreeSelectionEvent is used to notify TreeSelectionListener that the selection of a JTree has changed. This event will be generated when the user tries to edit or rename the topic node in the security topics tree of the GUI. As a result of this change in the topic name, a new Internet search will be performed and new results will be stored in the results file corresponding to this topic name, as well as displayed in the top frame of the right pane.

TreeModelEvent and TreeModelListener

The TreeModelEvent is used to notify TreeModelListener about the change in the TreeModel. The TreeModelEvent will be generated when a tree node is renamed, inserted, added, or removed and the TreeModel will be updated accordingly. For renamed, inserted, and added tree nodes, a new Internet search will be performed on those topics and the respective results file will be generated. The OASIS GUI display will be updated to reflect the change in the TreeModel.

HyperlinkEvent and HyperlinkListener

A hyperlink is an element in an html document that links to another place in the same document or to an entirely different document. Typically, a user clicks on the hyperlink to follow the link. The HyperlinkEvent is used to notify the HyperlinkListeners that something has happened with respect to a hypertext link. For the OASIS GUI, the hyperlinks, that are the results of an Internet search on a topic node, are displayed in the top frame of the right pane when the user selects that topic (leaf node) in the tree. The hyperlinks are highlighted in blue underlined text. If the user clicks on this link, a HyperlinkEvent will be sent to the HyperlinkListener. As a result, the web (or html) page that corresponds to this link will be displayed in the bottom frame of the right pane.

Notice that the bottom frame may have one or more similar hyperlinks. However, no HyperlinkListener is implemented to handle the HyperlinkEvent generated as a result of clicking these links. Therefore, the user will not notice any change in the GUI display.

ActionEvent and ActionListener

ActionEvent is a semantic event, which indicates that a component-defined action occurred. This high-level event is generated by a component (such as a Button) when the component-specific action occurs (such as being pressed). The event is passed to every ActionListener object that registered to receive such events using the component's addActionListener method. When the ActionEvent occurs, that object's actionPerformed( ) method is invoked.

Table A and B in Appendix A list all of the menu items and tool bar buttons supported by the OASIS GUI. An ActionEvent will be generated upon selection of each of these items and the appropriate action will be performed as described in the tables.

3.3 PROGRAM AND DATA FLOW

This section describes a general flow of data and control implemented in the OASIS software. It begins by reading the "topics.txt" file that contains the tree layout in the text format. Each line of text represents a node in the tree by a level number and name of the topic at that node. The level numbers and topics are stored in arrays. The tree is created by reading the level number and its corresponding topic name from these arrays and by comparing the current level number with the next level number in the tree to determine if the node is a parent or a child. At the same time, the Internet search is performed on the topic and the results are saved in the results file corresponding to this topic name.

An association is formed between the topic name and the results file by generating a user object, which is added as a topic node in the tree. The process can become time consuming depending upon the size of the "topic.txt" file or number of topics in the file. After the tree is created and all the results files are in place, the tree is displayed in the GUI along with the menu and tool bars.

Once the GUI is up and running, the ActionListeners and EventListeners described above will take over control and perform the necessary actions to update the GUI status. All of the data generated or needed by the OASIS application are stored in files. The tree content is in "topics.txt" file and the Internet search results on each topic are stored in the html file corresponding to each topic. Moreover, the downloaded html pages are also in separate html files. When a tree is modified in the GUI by user, the respective topics file or the results file will be updated or generated. The user can use any other name for the topics file after the application is started to save changes to the tree organization.

Create tree from text file

The difference between the values of the current and next level plays an important role in determining if the next node is a child of the current node or a child of a node a few levels up in the tree.

(i)   Initialize parentNode with the first topic in the tree (root)
and childNode be null

(ii)   For each topic in the text file

(iii)   Set currentTopic and let currentLevel be the level number corresponding to currentTopic in the file

(iv)   Set nextTopic and let nextLevel be the level number corresponding to nextTopic in the file

(v)   Check if ((nextLevel - currentLevel) = = 0) {
    // the topics at both levels are siblings
    //Parent of current node is same as parent of next node

    } else if ((nextLevel - currentLevel) = = 1) {
    // the current topics node is a parent and
    // the next topic node is a child

```
    } else if ((nextLevel - currentLevel) < 0) {
        // obtain the absolute value of the difference in level
        // go up that many levels and the topic at that node
        // is the parent of the topic at next level
    }
```

(vi)   Set the values for parentNode and childNode appropriately based on above condition checking

(vii)   Perform the Internet search on the topic using buddy search method and store the results in htm file

(viii)   Associate htm file with the topic

(ix)   Add the childNode to the parentNode

(x)   Adjust the values of childNode and parentNode

(xi)   Go to step (ii)

Create a text file from tree

A recursive tree traversal is performed to generate the text file format to match with the one used in the above section to create a tree from the text file. Depending upon whether the current child node is a leaf or a non-leaf node, it is important to increment or decrement the level number to accurately represent the level of that child, corresponding to its topic in the text file.

(i)   Starting with the root node as parent node, set level = 0

(ii)   Write the level and root name to the file

(iii)   For each child of the parent node, set the child node

(iv)   Increment the level number

(v)   If (child = = null)
        // Return from this path traversed from parent to the null child

(vi)   Write the level and child name to the file

(vii)   If (child.isLeaf())
                // Decrement the level number and continue
        else
        {
                // the child is a non-leaf (parent) node which has children of its own
                // Go to step (iii) to start traversing the path from this parent node to
                  all of its children
                // Decrement the level number to accurately represent the level of
                  child node
        }
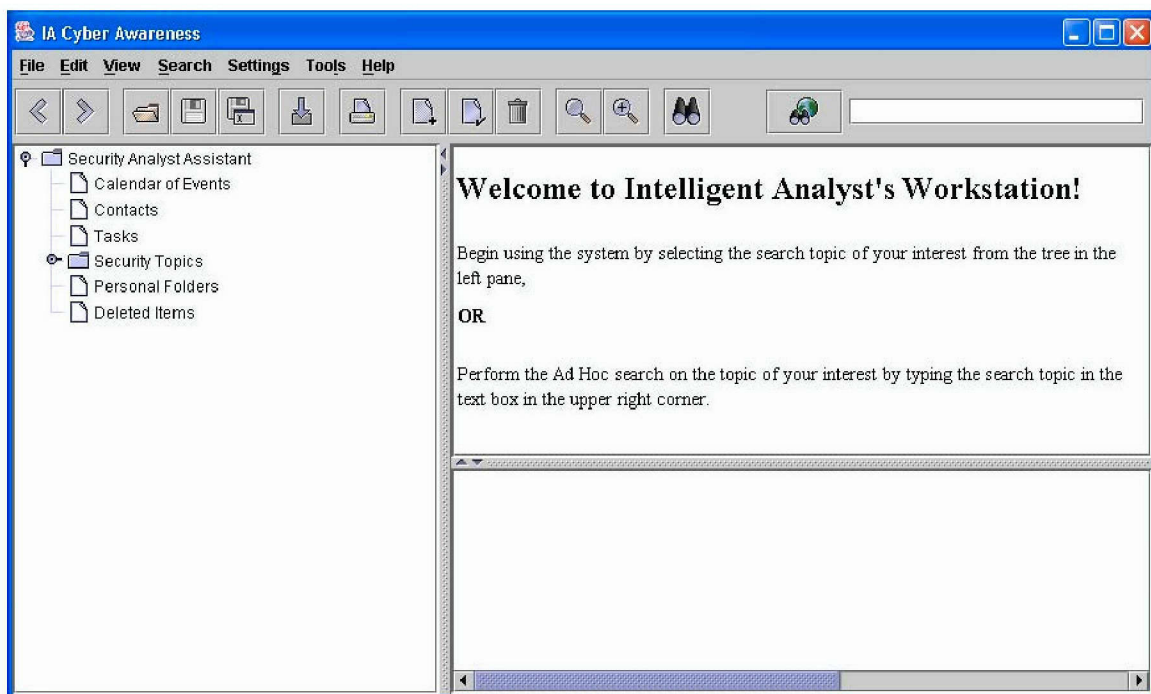
                                12
```

# 4.0  RESULTS AND DISCUSSION

This section presents the features and options of the OASIS software and discusses their use.

## 4.1  OASIS GRAPHICAL USER INTERFACE

Java-based GUI software was developed under this project.  Components comprising the GUI resemble Microsoft's Outlook application.  Designing the GUI to resemble Outlook was done mainly to reduce the time users would need to become familiar with this new tool.  Since most users are already familiar with Microsoft Outlook, the learning curve would be greatly reduced.  The main GUI window is divided into left and right panes, a menu bar, and a tool bar as shown in Exhibit 4-1.

Exhibit 4-1   The OASIS GUI



The left pane contains the tree organization of the security topics and other topics pertaining to collaboration of the security analyst's work activities.  The right pane is further divided into top and bottom frames.  The top frame displays the results of an Internet search on a security topic selected from the tree and is organized as a list of hyperlinks along with a brief summary of the information contained in the web page corresponding to that hyperlink.  The bottom frame displays the contents of the web page corresponding to one of the hyperlinks selected from the top frame.  Notice in our example that none of the hyperlinks in the bottom frame are activated.

The menu bar provides options for different operations that can be performed from the GUI. These options are grouped based on the type of operations that can be performed on the GUI components. The menu bar also provides the keyboard shortcuts for most of the menu options. This feature is handy in the absence of a mouse for input selection.

Many of the menu bar options are provided along with meaningful graphical icons in the tool bar. The key difference is that the tool bar options need a mouse device for selection. Compared to menu bar options, the tool bar requires a single mouse click to perform a specific operation whereas the menu options require at least two mouse clicks, depending upon the depth of the menu options.

## 4.2  BUDDY INTEGRATION

Buddy is a meta search engine that uses a combination of Google, Yahoo, and other similar search engines to assist the user in advanced search and collection of information from the Internet. It provides the necessary tools and flexibility to quickly organize your ideas, search for multiple items from a number of sources and combine the results into a single set. It is a Government Off-The-Shelf (GOTS) product developed at AFRL Rome Research Site (RRS) and is freely available for leverage.

One of the key features that is readily leveraged is the ability to add or remove and to configure the data sources (e.g., web sites such as Yahoo, Google, SNORT, CERT-CC, and Security Focus). The configuration of data sources involves setting up variables in Buddy depending upon the search mechanism used by the individual web site. For example, for a search on the phrase "Top Ten Vulnerabilities", GOOGLE appends "search?hl=en&ie=UTF-8&q=%22Top+Ten+Vulnerabilities%22" string to its base URL http://www.google.com. For the same search Yahoo appends "search?p=%22Top+Ten+Vulnerabilities%22&ei=UTF-8&fr=FP-tab-web-t&cop=mss&tab=" to its base URL http://search.yahoo.com. If these web sites change anything in its search mechanism, then the user has an option to manually fix the source. Alternatively, Buddy can be trained to automatically fix the source.

To take advantage of such capabilities, a very minimal Buddy integration is performed. Essentially, when a user requests a search on a security topic, the GUI prepares the format in which the Buddy method will accept the search string. It obtains the list of URLs returned by the Buddy method and displays them in the top frame of the GUI's right pane. The user must install Buddy along with the OASIS software in order to configure Buddy for security web sites and other basic Internet-related settings. As a result, the Buddy configuration options are not implemented in the OASIS GUI, though they are mentioned in the OASIS GUI for completeness.

## 4.3  MANUAL DOWNLOAD OF HTML PAGES

Downloading an html page brings a local copy to the user's computer. This is the page that is accessed when the Internet is on-line and user selects a link to that web page. The OASIS GUI provides the option to download all of the html pages corresponding to the links in the results file

generated for each search topic in the tree. This operation is time-consuming, especially if there are many topics in the tree. A tool bar button and a corresponding file menu option are provided so that the user can initiate automatic download of the pages without manually printing each page. This operation must be performed at least once before the Internet goes off-line.


## 4.4  INTERNET ON-LINE AND OFF-LINE SUPPORT


The ability to download html pages makes it possible to continue using this system when the Internet is off-line. How current the information is at that point depends upon the last time the download was performed. The system is fully functional when the Internet is available.


## 4.5  SEARCH FLEXIBILITY


If the user changed the tree organization by adding new security topics or renaming the topic while the Internet was off-line, the results file will not be generated for the new topics. With the "Search Selected Topic" option available as a tool bar button and as a menu item, it will be possible for the user to go back and search the web for new topics when the Internet is back on-line. At any other time, this option can be used to obtain the latest or updated information on the web about any of the security topics. Also, the "Search All Topics" option can be used to get the latest information on all of the security topics in the tree.


## 4.6  ORGANIZING SECURITY TOPICS


Because of the organization of the security topics in the tree structure, it is possible to expand the tree efficiently and easily. It is also a better choice for a system of this nature.


## 4.7  SAVING AND OPENING FILES


It is possible to save the file to the same or to a different text file after modifying the tree in the GUI. Modifying the tree in the GUI is easier than counting the level numbers for the topics and editing the text file. If the tree is greatly modified, then it can be saved under a different name to distinguish the changes from the original file. Also, if the user wishes to use the security topics organization used by another security analyst because it represents a better collection of topics or association, then the user can simply open that file in the GUI and start using it.


## 4.8  ADHOC INTERNET SEARCH


If a user wants to quickly look up a topic that is not part of the security topics tree but doesn't care to maintain the search results on this topic, nor download the html pages for the results, then

the user can use the "Adhoc" search option. The topic could be a word or a phrase that the user came across while reading through any of the search results.

## 4.9  DOCUMENTING THE TREE STRUCTURE

Use of text file makes the system platform independent and easier to create and edit the file using any of the simple editor programs such as Notepad, Wordpad, Textpad, etc.

## 4.10 LIMITATIONS

1.  It is not possible to download the html pages for a single topic. This operation must be performed for all of the security topics. The main reason for providing this option is to allow operation to continue in the event that the network goes down and the Internet goes off-line.

2.  The system does not automatically perform the periodic Internet search on all of the topics to inform the user about the latest updates. However, modules like "Search Selected Topic" or "Search All Topics" are in place to provide this functionally with a minor addition of time function.

3.  The data base is not used to store search results information but relies on the file system on the host machine.

4.  The hyperlinks in the bottom frames are not activated. The frame simply displays the content of the html page corresponding to the hyperlink URL.

5.  Multi threading is not implemented therefore it makes the program execution sequential, particularly when the "Open" file operation is performed. Depending upon the number of topics in the file, it can take noticeably longer for the GUI to respond to this request since the Internet search is performed on each topic as it is read from the file. Similarly, with "Download html pages", it takes even longer as it tries to download the web page for each individual link in the results file corresponding to each topic in the tree. The workaround is to wait while performing such an operation until the user finds a break when s/he is not going to use the system during that time.

6.  Minimal Buddy integration is performed. The user will have to use the Buddy GUI in addition to the OASIS GUI to use other Buddy features such as configuring and adding new data sources or search engines.

# 5.0 CONCLUSIONS AND LESSONS LEARNED

The cyber threat, vulnerability, and countermeasure information needed for securing an organization's network is available on the Internet in many different forums. For example, the information on network security products is published by vendors such as Symantec and McAfee; guidelines and procedures related to network security incidents and recovery information are published by groups such SANS, CERT/CC and W3C; operating systems and applications-specific vulnerabilities and information on patches is put forth by companies such as Microsoft and Linux.

An effective information search on the Internet is difficult without a tool that lets the user customize the search and retrieval process. The OASIS software attempts to provide this capability in a user-friendly GUI environment with the added flexibility of organizing the search topics and downloading the search results. These features can helpful when the Internet is not available.

Effective information extraction is another feature that processes the data retrieved as a result of the Internet search. It organizes, combines, and summarizes the data to make them specific to the search topic and presents them in a prioritized order with the reference links made available for further help. The OASIS software has been developed with these requirements in mind and includes software components that could be modified and enhanced to provide the features for information extractions. Initially, it will require more research and investigation to find the tools that currently provide some or all of the requirements for extraction. The possibility of integrating these tools with OASIS or conducting a scientific study to design algorithms to accomplish effective information extraction can also be explored.

# 6.0 RECOMMENDATIONS

Here are the recommendations we formed based on our work on OASIS.

## 6.1 INFORMATION EXTRACTION

It is recommended that various methods/tools (COTS or GOTS) developed in the area of information extraction be investigated and evaluated. With the limited research conducted thus far, we have learned that the Intelligence Community has some primitive tools to assist with situation awareness in the areas of drug trafficking, terrorism, WMD (Weapons of Mass Destruction), etc. These tools work on text documents and extract information such as Names, Locations, Dates, Organizations, and Event. This information can be processed further using the tools that map the relations among these entities and show the connection among the people, places, and organizations with the events.

For the information extraction in network security domain, some of the information such as known attacks and patches in the html documents (i.e., web pages such as SNORT, CC/Cert, Symantec, etc.) can be in the form of tables or lists (which are already organized based on some derived relationship). Therefore, the tools mentioned above will not be suitable for a network security domain. However, information such as the latest security news will be in the form of an article or stream of text, which might contain information on newly formulated attacks, etc. Even for such information, the extraction could be simply capturing all of the text around the search topic that would have the potential information about the attack.

No single information extraction technique will work for all of the types of information in a network security domain that we attempted to provide in the OASIS software. Therefore, it is recommended that the one that covers the majority of information types be explored first.

### 6.1.1 FETCH TOOL

A COTS product from Fetch Technologies (referred to as the Fetch tool) has some potential applicability in network security domains. The tool works very well with static web pages. These pages are static because the location of the information on the web page is fixed. For example, the top ten vulnerabilities are posted on the Symantec web site in tabular format. As new vulnerabilities are discovered or the severity level changes, the table will show updated information but will still be positioned in the same place on the web page. The Fetch tool is very suitable for this type of information because the user can train the tool to return periodically to this table for the latest vulnerability information. There is always the possibility that Symantec could reorganize all of its information or shift to a new web server but changes of this nature are not expected to be frequent.

It is recommended that further evaluation of the Fetch tool be conducted to determine the areas of information in the network security domain that use static web pages for extraction of

information. It is also recommended that the possibility of obtaining the application programming interface (API) from the company be explored and then estimate the effort that would be required to integrate it with the OASIS GUI.

## 6.1.2  INTELLIGENT INFORMATION RETRIEVAL

Dr. Eugene Santos, the Director of the Intelligent Distributed Information Systems Laboratory at the University of Connecticut, recently presented some of his research work in the intelligent information retrieval field at AFRL/RRS. It is recommended that a follow-up be conducted with Dr. Santos to explore the possibilities of leveraging his research work to apply it to information extraction in a network security domain.

## 6.2  SOURCE CODE UPGRADE

The following upgrades to the existing OASIS software are recommended.

1. Modularize the code. It is important to separate the back-end and front-end functionality from this single large program as well as to classify the appropriate methods for the relevant classes. This will greatly increase the code reusability and ease future modifications.

2. Add support for threading. For better GUI response time, a separate thread should be created for each of the time-intensive GUI operations requested by the user that involve lengthy Internet search and retrieval work.

3. Add capability to drag and drop the search results into a "personal folder" or a "deleted items folder".

4. Notify the user about the latest security updates by displaying a flag in the GUI near the relevant security topic or with a pop-up message dialog.

## 6.3  GUI MODIFICATION

As a result of the above-recommended enhancements to the OASIS software, the user interface will need to be upgraded to reflect the proper presentation of extracted information.

## 6.4  TECHNOLOGY TRANSITION OPPORTUNITIES

Even though the OASIS software focuses on the network security domain, the tool is generic as it will be applicable to other information domains with minimal modification to the information extraction part. Without any modification, the tool will return the information specific to other

domains but it may not be customized to suit the amount and presentation of information in other domains.

# APPENDIX A
## SOFTWARE USER'S GUIDE

This section describes the system usage with the help of various screen shots and detailed steps. It also specifies the actions that are allowed and not allowed.

1. GUI Welcome Page

   This is the first page displayed when the application is started. It contains the application title in the top left corner, menu bar, and tool bar. The top right pane displays the welcome message and prompts the user to begin using the application by selecting the appropriate topic from the tree in the left pane. The partially expanded tree in the left pane is the fixed part of the tree that cannot be modified by any of the following actions:

   a. Rename topics at the root node or its children

   b. Deletion of root node or its children

   c. Add (children) or Insert (siblings) nodes to root node

   d. Insert another root node (sibling of root node)

2. Selection of the topic at non-leaf node of the tree

As a result of this action, the list of the selected node's leaf or non-leaf nodes will be displayed in the top frame of the right pane.

3.  Selection of the topic at the leaf node of the tree

    Displays the results of the Buddy search performed on the topic at the selected node in the form of a list of html links (Result 1, Result 2, etc.) ordered by the search engines (AltaVista, Google, etc.) in the top frame of the right pane.

Selecting one of the links from the results will display the web page corresponding to that link in the bottom frame of the right pane.



4. Add a topic node

Select a tree node to which you wish to add a topic node. Then select the tool bar icon  or from the menu bar choose <Edit> followed by the menu item <Add Node>. This will prompt you to "Enter New Topic…" Provide the appropriate label for the new topic node and hit <OK>. At this point, you have an option to cancel this operation.

Note that the new node is added as a last child of the selected node. The "Denial of Service Attacks" topic is added to the "Latest security news" node as its last child.

As a result of this operation, the Buddy search will be performed on the newly added topic and the results will be available for display in the right pane.



5. Insert a topic node

Select a tree node in which you wish to insert a topic node. Then select the tool bar icon or from the menu bar choose <Edit> followed by the menu item <Insert Node>. This will prompt you to "Enter Topic String…" Provide the appropriate label for the new topic node and hit <OK>. At this point, you have an option to cancel this operation.

Note that the inserted node is added as a sibling of the selected node. The "Incident Reports" topic is added to the "Latest security news" node as its sibling.

As a result of this operation, the Buddy search will be performed on the newly inserted topic and the results will be available for display in the right pane.

6. Delete a topic node

Select a tree node that you wish to delete. Then select the tool bar icon 🗑 or from the menu bar choose <Edit> followed by the menu item <Delete Node>. This will prompt you for the confirmation of deletion. At this point, you have an option to choose <Yes>, <No>, or <Cancel> this operation.

If you chose to continue deletion, the node will disappear from the tree.

7. Rename a topic node

Double click on the tree node that you wish to rename. The node will appear as shown in the screenshot below to allow you to edit the text. Note there is no tool bar or menu bar option to perform this operation. Rename "Incident Reports" to "Incident Notes" and hit <Enter> after you finish typing.

As a result of this operation, the Buddy search will be performed on the renamed topic and the results will be available for display in the right pane.

8. Search selected topic

Select a tree node on which you wish to obtain the latest security information. Select the tool bar icon 🔍 or from menu bar choose <Search> followed by the menu item <Search Topic>. If the selected node is a non-leaf node (e.g., "Latest security news"), you will be informed that the search cannot be performed on non-leaf node. If a leaf node was selected, then depending on the time elapsed between the last search and this search, the results will differ.



9. Search all security topics

Perform this operation by selecting the tool bar icon 🔍 or from the menu bar choose <Search> followed by the menu item <Search All>. This is similar to Windows Operating System's "Refresh" operation. It will result in performing the Buddy search operation for all of the topics at the leaf nodes in the subtree that falls under "Security Topics" node of the tree.

## 10. Adhoc search

This is a one-time search that you may wish to perform on a security topic that is not part of the tree. It may be used to find another reference from which to learn additional information about the original topic, or information on another topic in the tree, or just a quick search on a random topic.

Type the search topic in the text box provided at the upper right corner of the GUI window and hit tool bar icon ![icon] when you are ready to begin the search. The results will appear in the top frame of the right pane. If you select any of the links in the search results, then the web page corresponding to that link will appear in the bottom frame of the right pane.

11. Open file

Open a text file containing a different search topics organization named "iran1.txt". To perform this operation, select the tool bar icon 📂 or from the menu bar choose <File> followed by the menu item <Open…>. You will be prompted to type the file name.



You can open an existing file or create a new text file by specifying the root of the topics tree with level number "0" followed by "comma" followed by its "label". Then increase the levels of the rest of the topics in the tree depending on where in the tree structure that topic will appear. The text file looks like this and is the required format for the text file. It will not allow blank spaces before and after "comma", at the "end of the line", or at the "bottom of the file".

Notice in the screenshot below that the fixed part of the tree is unchanged with the opening of a new file but the new topic tree from the file appears under "Security Topics" node.



12. Save file

To the above tree organization of iran1.txt file, modify the topics tree by adding a subtree with the parent node "Natural resources" and children nodes "Oil" and "Soil".

To perform this operation, select the tool bar icon ⊟ or from the menu bar choose <File> followed by the menu item <Save>. The Save File operation will save the changes to "iran1.txt" and the text file will now look like this.



13. Save file as

Modify the tree content again by deleting some topics from the tree such that it looks like the screen below.

The Save As operation will prompt you to save the tree topics under the Security Topics node with a different file name. Type the new file name as "iran2.txt".



Notice that the content of "iran2.txt" will now look like this.



14. Download html pages

To perform this operation, select the tool bar icon  or from the menu bar choose <File> followed by the menu item <Download files>.

There is always the possibility of a network going down for various reasons. This option for downloading html pages is provided to allow the user to save the html pages that correspond to the html links returned by the Buddy search on each of the topics under the "Security Topics" node of the tree. Because this operation could take a long time to complete, it is

recommended that the user start it when normal usage of this application is not affected., e.g., before going home for the day, during a lunch break, etc., though it is important that this step must be performed before a network goes down. In this situation, the downloaded pages will be useful to continue using the application for its intended purpose, even thought the network is temporarily unavailable. The downloaded pages could also be used on a machine that is not on the network The data will be as old as the last time the download was performed.

## 15. Menu bar Summary

The table below summarizes the menu items along with descriptions for quick look-up.

### Table A.   Menu Bar

| Main Menu | Submenu | Shortkey | Comments |
|---|---|---|---|
| File | | Ctrl-F | |
| | Open… | Ctrl-O | Open an existing security tree |
| | Save | Ctrl-S | Save the tree under same name |
| | Save As… | Ctrl-A | Save the tree under a new name |
| | Download files | Ctrl-D | Download all html pages |
| | Print | Ctrl-P | *Not Implemented* |
| | Exit | Ctrl-X | Exit the application |
| Edit | | Ctrl-E | |
| | Add Node | Ctrl-D | Add node as a child of current node |
| | Insert Node | Ctrl-N | Add node as sibling of current node |
| | Delete Node | Ctrl-L | Remove current node |
| View | | Ctrl-V | |
| | Toolbar | - | Display or hide the tool bar |
| Search | | Ctrl-S | |
| | Search Topic | Ctrl-T | Search Internet on current node |
| | Search All Topics | Ctrl-L | Search Internet on all security topics |
| Settings *(Not implemented - Use buddy application)* | | Ctrl-G | |
| | Search Interval… | - | Specify the time for periodic search |
| | Configure Source… | - | Edit the data source settings |
| | Preferences… | - | Internet and search engine settings |
| | Select Sources… | - | Select data sources i.e. web sites |
| Tools *(Not implemented)* | | Ctrl-L | |
| | Find | - | Find keyword in personal folders |
| | Empty "Deleted Items…" | - | Remove deleted items node content |
| | Restore "Deleted Items…" | - | Restore deleted items node content |
| Help *(Not implemented)* | | Ctrl-H | |
| | About | Ctrl-A | Display application version info |

## 16. Tool bar Summary

The table below summarizes the tool bar icons along with descriptions for quick look-up.

Table B.   Tool Bar

| Icon | Description |
|------|-------------|
| | Back to previous results page  *(Not implemented)* |
| | Go to next results page *(Not implemented)* |
| | Open topics file |
| | Save changes to current file |
| | Save changes to another file |
| | Download html files corresponding to the search results for each security topic |
| | Print html pages in the bottom frame of the right pane *(Not implemented)* |
| | Add new topic node as a child of the current node |
| | Add new topic as a sibling of the current node |
| | Remove the current node |
| | Perform Internet search on the security topic at the current node |
| | Perform Internet search on all of the topics under "Security Topics" node |
| | Find a keyword in the personal folders *(Not implemented)* |
| | Perform a one time search on any of the security topics |

# APPENDIX B
# BIBLIOGRAPHY

Robinson, Mattew, and Vorobiev, Pavel. *Swing*. Manning Publications Co., 2003.

Sun Microsystems. "Java 2 Platform, Standard Edition, v 1.4.2 API Specification". Available from http://java.sun.com/j2se/1.4.2/docs/api/index.html. Internet, accessed 30 September 2004.

Sun Microsystems. "Java look and feel Graphics Repository, Technical Articles and Tips". Available from http://java.sun.com/developer/techDocs/hi/repository/. Internet, accessed 30 September 2004.

Sun Microsystems. "The Swing. Tutorial, Trail: Creating a GUI with JFC/Swing". Available from http://java.sun.com/docs/books/tutorial/uiswing/. Internet, accessed 30 September 2004.